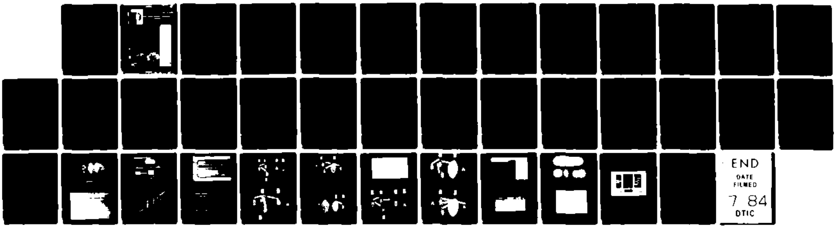
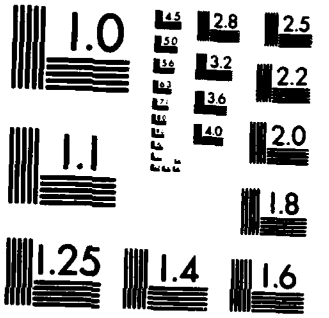
AD-A141 282 A FULLY DISTRIBUTED APPROACH TO THE DESIGN OF A 1/1
KBIT/SEC VHF PACKET RADIO..(U) ROYAL SIGNALS AND RADAR
ESTABLISHMENT MALVERN (ENGLAND) M S HAZELL ET AL.
UNCLASSIFIED FEB 84 RSRE-84003 DRIC-BR-91513 F/G 17/2.1 NL



END
DATE
FILMED
7 84
DTIC



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

ROYAL SIGNALS AND RADAR ESTABLISHMENT

Report No 84003

Title: A FULLY DISTRIBUTED APPROACH TO THE DESIGN OF A 16 KBIT/SEC VHF PACKET RADIO NETWORK

Authors: M S Hazell and B H Davies

Date: February 1984

## SUMMARY

System design considerations for a Packet Radio network operating in the mobile tactical environment are outlined. Survivability is assessed to be of primary importance and a fully distributed approach in which all nodes are functionally equivalent and the network self-configuring is favoured. Emphasis is placed on a description of the channel access (CA), routing and congestion control algorithms. The CA algorithm is an adaptive CSMA scheme which is designed to maintain good throughput-delay performance irrespective of the number of active users and offered loading. It specifically includes features which compensate for 'hidden terminal' effects in multiple hop networks. The routing strategy takes advantage of the inherent path redundancy of the semi-broadcast environment to offset the high packet loss rate due to collisions, interference and fading. Highlighted are those aspects which ensure effective routing in the face of rapid topological change and consequent out-moded routing data. Algorithm development has been aided by computer simulation using a finite state machine technique to model a realistic network of up to fifty nodes. This is described and results are presented which characterise the performance of networks with various topologies. Finally there is a brief description of a prototype applique unit which allows a conventional tactical VHF transceiver to be adapted for use as a Packet Radio unit.

# ' A Fully Distributed Approach to the Design of a 16 kbit/sec VHF Packet Radio Network

by

M.S.Hazell and B.H.Davies

System design considerations for a Packet Radio network operating in the mobile tactical environment are outlined. Survivability is assessed to be of primary importance and a fully distributed approach in which all nodes are functionally equivalent and the network self-configuring is favoured. Emphasis is placed on a description of the channel access (CA), routing and congestion control algorithms. The CA algorithm is an adaptive CSMA scheme which is designed to maintain good throughput-delay performance irrespective of the number of active users and offered loading. It specifically includes features which compensate for 'hidden terminal` effects in multiple hop networks. The routing strategy takes advantage of the inherent path redundancy of the semi-broadcast environment to offset the high packet loss rate due to collisions, interference and fading. Highlighted are those aspects which ensure effective routing in the face of rapid topological change and consequent out-moded routing data. Algorithm development has been aided by computer simulation using a finite state machine technique to model a realistic network of up to fifty nodes. This is described and results are presented which characterise the performance of networks with various topologies. Finally there is a brief description of a prototype applique unit which allows a conventional tactical VHF transceiver to be adapted for use as a Packet Radio unit.

## I. INTRODUCTION

The increasing use of computer based equipments in weapons systems and their associated sensors and command and control elements and the trend from voice to data communications have been responsible for formulating the requirement for robust data communications systems for use in the Forward Area Tactical Environment. This paper describes the philosophy, design and performance of a fully distributed medium speed Packet Radio network for providing survivable data communications in a hostile electromagnetic environment. A major advantage of this approach is that it can be used with current combat net radio transceivers using the same frequency band and modulation as is currently used for digitized voice. Thus the user is already familiar with the link performance of the proposed network; a particularly important point in view of the fact that the topology of the Packet Radio nets is determined by non-communications operational requirements.

Packet Radio research and development has been pioneered in the US since 1973 by the Defence Advance Projects Agency. The Experimental Packet Radio Programme [1] not only has the capability to accommodate hundreds of users on a single channel, but also offers very short network transit delays of the order of a hundred milliseconds. These parameters dictated a shared channel capacity of 100-400 kbits/sec, which at the carrier frequencies employed necessitates a backbone of well-sited or airborne repeaters. Our work in Packet Radio is essentially complementary to this programme in that both the numbers of users and the shared channel capacities are an order of magnitude smaller. The consequent use of the low VHF band greatly reduces the line-of-sight problems, and permits a completely non-hierarchical approach.

Our approach to the design has been necessarily heuristic since we believe it is important to consider as realistic a network as possible and this means excluding the significant simplifications which are required in order to make analysis tractable. The design as it now stands has evolved through and been tested by extensive computer simulation using a finite state machine representation with the controlling algorithms operating independently for each modelled unit. Despite the heuristic approach, much reference has been made to literature [2,3,4,5] on the analysis of similar but simplified systems and many aspects of the design are practical extensions of well researched techniques.

### A. Philosophy of a fully-distributed approach

If a Packet Radio network relies for its operation on the controlling influence of a number of specially equipped station units then the survivability of the entire network is effectively compromised by the vunerability of these individual units. In particular , if the stations are in any way distinguishable by the enemy then they will be made the focal point of any physical or electromagnetic attack on the network. Even excepting this , the implication of their chance destruction or failure must still constitute a serious weakness.

The vulnerability is clearly greatest for single station control and reduces as the number of stations is increased. Further reduction can be effected if the number of units having the potential to act as stations is greater than the number of active stations such that losses can be repaired. However, if a unit is to perform a station function then it must be deployed in a selected location with reasonable connectivity wheras it would be preferable from logistical and operational grounds if deployment were totally flexible. On these grounds it would be advantageous if all Packet Radio units were identically equipped.

At this point it is pertinent to question the need for station control in the normal sense. If all the units are made identical and intelligent then complete distribution of control becomes a possibility. That is we may consider a 'stationless` approach. This is particularly appropriate in medium-sized networks for which the volume of control information is not too great. Our use of a 16kbit/sec channel means that we are naturally limited to medium-sized networks (<=50 units) and so this is a complementary constraint. Our belief is that, whilst full distribution may not offer quite the efficiency of a well engineered hierarchical approach, the benefits in terms of enhanced survivability are highly desirable in the Forward Area communications environment.

## II. BASIC CONCEPTS OF A NON-HIERACHICAL PACKET RADIO NETWORK

A Packet Radio Network consists of a number (<=50) of microprocessor controlled radio-transceivers that share a single channel to exchange discrete units of data called packets. A packet consists of a few hundred to a few thousand bits of user data with some identification and control information in a header. Each Packet Radio unit is not necessarily in direct radio contact with all other units and packets may be relayed to their destination in a number of hops. In order to provide this relaying function in an automatic and efficient manner each station maintains its own picture of the topology or layout of the network from control packets that it receives from its neighbours and from data packets in transit. These concepts are illustrated schematically in Figure 1.

The single channel does not necessarily imply a single carrier frequency, a net could be based upon a frequency-hopped channel if this was a desired ECCM technique. Two very important features of Packet Radio nets are the channel sharing algorithm which should be capable of efficiently sharing the available capacity equitably or in some other required priority between the active users, and the automatic routing algorithm which adapts to the mobility of the users and to changes in the electromagnetic environment.

There are a number of unique problems associated with the design and mode of operation of such a Packet Radio network. These differences between Packet Radio and other broadcast and link networks result in the need for new types of algorithms for network control and routing. The unique aspects of Packet Radio networks include:-

1) HIGH PACKET LOSS RATE - which can be as high as 5 to 70% for two reasons. Firstly, high bit error rates are common in the mobile tactical environment (10-3 to 10-1) due to multipath fading, local obstructions, ignition interference and jamming. Although forward error correction techniques can be used to reconstruct packets with limited numbers of errors, some packets will inevitably be beyond repair. Secondly, by the nature of the commonly used contention-based access procedures, clashes occur between two or more transmitters especially at high traffic loadings. The amount of clashing also depends upon the topology of the network in that two transmitters out of contact with each other may both illuminate a number of other units thus causing frequent clashes to the jointly illuminated units (the 'hidden terminal` problem).

2) THE SEMI-BROADCAST NATURE OF TRANSMISSIONS - (i.e. a transmission by one unit may be received by a number of neighbour units), this feature means that there is an inherent redundancy in the basic mode of operation which can be used to compensate for the high packet loss rates described above.

3) HIGHLY DYNAMIC CONNECTIVITY - because of the mobility of the users/transceivers and because rapid and significant changes in the electromagnetic environment are possible especially in an hostile environment.

## A. Features of a Packet Radio Network

The primary function of a Packet Radio network is to provide a stated grade of data communications service between its users. This grade of service may be defined in terms of availability, throughput, average delay and delay dispersion. In performing this primary function a Packet Radio network should exhibit the following attributes to the user:-

Automatic flexibility

A Packet Radio network should be totally flexible in the manner in which it shares out the available channel capacity in that if there are two users they are each able to have at least 50% of the sharable capacity while if there are 50 users they are able to have at least 2% of the sharable capacity and the adaption between these conditions should be rapid and automatic. Furthermore the network should configure itself automatically on switch-on without having to have any 'a priori' knowledge of connectivities, and continuously adjust to changes in connectivity (i.e. make the best use of the prevailing connectivities).

Interoperability

An efficient automatic internetworking capability provides two types of service enhancement. Firstly it permits fast and efficient access to information which may be held on databases on other networks, which with the advent of satellite surveillance and more sohpisticated battlefield monitoring techniques will become increasingly required. Secondly, a richly interconnected internet system can be used to enhance survivability of communications on a single net as described below. The use of a properly layered-protocol architecture enables easy and efficient implementaton of internetworking protocols in all Packet Radio stations [6].

Survivability

The grade of service and capacity of a Packet Radio network should degrade gracefully upto the point where there does not exist any radio connectivity between two or more subsets of the users. Even when the network has become partitioned members of different partitions may still communicate if the network has a number of gateways to an internet system. Initially, this may mean that networks which have wide geographic distribution may have a number of gateways into a trunk network so that, should they become partitioned, the partitions could continue to communciate via the trunk network.

Cost-effectiveness

It is essential, whatever the merits of the system, that it be affordable by the users. The work described in later sections indicates that Packet Radio networks could be provided in the medium term by building an adaptor or applique unit to combine with a current combat net radio (CNR) transceiver thus permitting Packet Radio to be introduced gradually and cheaply.

## III. SYSTEM DESIGN

A summary list of the design considerations are given in Figure 2.

### A. Type and Grade of Service

As the system design is as far as possible scenario and threat independent, a number of different types of service are provided:-

1) 'UNRELIABLE DATAGRAM' - these are used to transport time-perishable data such as radar plot information, where

timeliness of delivery is more important than reliability.

2) ACKNOWLEDGED DATAGRAM - these are use to transport highly formatted information which may be fitted into one packet. These messages may require either acknowledgement of delivery or a reply which implies delivery. Such messages can use an acknowleged datagram service.

3) VIRTUAL CALL - this is used to provide reliable ordered delivery of a stream of data with the associated flow control which necessitiates the use of a powerful end-to-end protocol such as the DoD TCP (Transmission Control Protocol)[7].

4) INTERNETWORK SERVICE - the capability for communicating with hosts on different types of networks can be provided by use of the DoD IN protocol (InterNetwork protocol)[8].

The grade of service required will depend very much on the application. For example an artillery fire control net may require deliveries in a few hundred milliseconds and thus such a net would have a relatively low activity level and involve a small number of hops. While a general logisitic support net may require high throughput but delays of upto ten seconds may be acceptable. The type and grade of service coupled with the number of active users determines the sharable capacity required. The capacity combined with the modulation requirements, such as robustness to multipath fading, determine the frequency band and bandwidth required. The ability to coexist with current combat net radio users (i.e. use same channel spacing) is also a highly desirable feature. From the above considerations potential users have indicated that the majority of applications for data transfer in the forward area environment can be catered for by use of medium speed Packet Radio net based on a shared 16kbit/sec channel.

The remaining design considerations are discussed in detail in the following sections except those pertaining to the user interface. A special feature provided by the user interface is a network management aid concerned with topology. Topology has not been included in Figure 2 because it is not primarily under the system designer's control. In the forward area tactical envrionment the geographical layout of the radios is determined by the functions being carried out by the units. Thus the network is designed to be selfconfiguring without any a priori knowledge of the connectivity of the net. However, it is possible that the layout will fail to support the data transfer requirements of the users. A priveleged command may be entered at any terminal which will result in the display of connectivity and traffic loadings of the network, thus enabling a Signals Officer to minimally perturb the locations of some users to obtain the required performance.

## IV. CHANNEL ACCESS

### A. Access control

Access to the shared channel is by non-persistent CSMA , chosen because of its suitabitity for demand assignment under distributed control and in view of its performance capabilities with achievable receive to transmit switching times. However , at sufficiently high total offered load the throughput falls to zero [2] and consequently one of the major problems of its practical application is in the design of distributed control procedures to prevent entry into this unstable region. In fact it is generally desirable to limit the offered load at some point below that at which the maximum throughput occurs such that the delay performance can be improved. This is the basis by which a trade-off can be made between throughput and delay performance. The chosen operating threshold will depend on the type of usage required of the network and is intended to be a configuration parameter.

In addition to the need to limit the overall system input rate it is also beneficial to control the time distribution of input . This is because CSMA systems are best suited to input which consists of short bursts of data separated by random inter-arrival times . Clearly it cannot be left to the users of a tactical communications system to ensure that these requirements are met when failure to do so could result in extreme degradation of performance. For these reasons we have designed control algorithms which allow the system itself to control when access attempts may be made and consequently when new user-input may be accepted. Each unit generates scheduling events and it is only at the instant of a schedule that a unit is permitted to attempt to access the channel (assuming that it has a packet to transmit) in accordance with the non-persistent CSMA protocol. There are two types of schedule which we refer to as 'continuous` and 'special`. The continuous scheduler is dominant and runs at a rate determined by an adaptive algorithm.

### Continuous Scheduler

This is a constantly running 'daisy-chain` scheduler and is the primary means of controlling channel access. It produces scheduling events which are spaced by uniformly randomised time intervals in the range from zero to a maximum as specified by the parameter 'schedint` (Ts). This gives an average rate of one schedule every Ts/2 time units. Each Packet Radio unit runs its own scheduler with its own value of Ts. This mechanism randomises the time distribution of system input and, more importantly, imposes a maximum input rate for each unit and consequently the system as a whole. In this way it provides an essential decoupling between the system and external events as generated by its users. The parameter Ts is calculated on the basis of monitored channel history data by the adaptive algorithm which is described presently. This is the basis of the distributed control of the total load offered to the channel (Figure 3).

Although this scheduler will generally run continuously there are occasions when it is useful to reset it. At present we allow it to start again with an immediate first schedule if a new packet is input by the user at a time when there are no other packets queueing at the unit. This modification is most significant at low loading and was introduced as a means of reducing pre-transmission delays.

### Adaptive Scheduling Algorithm

Over an integration period T each node monitors the channel and records the number of packets received correctly Nr and the number of detected clashes Nc. At the cessation of this period the control algorithm is called.

The channel history data Nr and Nc is used to calculate the percentage 'clash-ratio' as given by,

$$\mathrm{clashratio} = ( Nc / (Nr + Nc) ) *100\% .$$

This is compared with a system control constant 'clash-control' which is the value of the clash-ratio corresponding to optimal channel loading (found empirically) On the basis of this comparison one of three control actions is taken.

i) clashratio > clashcontrol<br>
Action: increase Ts<br>
Ts = Ts + errorfactor (Ts max - Ts)/8

ii) clashratio < clashcontrol<br>
Action: decrease Ts<br>
Ts = Ts - errorfactor (Ts - Ts min)/8

iii) clashratio = clashcontrol<br>
Action: none

The errorfactor, Er, is given by

$$Er = \begin{cases} \dfrac{\text{clashratio-clashcontrol}}{\text{clashcontrol}} & \text{for } \dfrac{\text{clashratio-clashcontrol}}{\text{clashcontrol}} < 1 \\ 1 & \text{for } \dfrac{\text{clashratio-clashcontrol}}{\text{clashcontrol}} >= 1 \end{cases}$$

The control actions provide negative feedback. If the detected clashratio is too great and , therefore, the channel loading too high then the unit reduces its scheduling rate and hence reduces its contribution to the overloading. Conversely, if the detected clashratio is too small then the unit increases its scheduling rate.

The value of Ts is confined to fall between the preset minimum and maximum limits , Ts min and Ts max. The algorithm allows Ts to move towards the required extreme by a fraction of its separation from that extreme. This means that the available movement is generally asymmetrical with greater possible travel towards the further extreme, as illustrated in Figure 4. This feature was found necessary to prevent an alternative but undesirable system state in which a few 'greedy` users took control of the system with rapid scheduling whilst the other users were locked out with slow scheduling. With the present algorithm such a situation is inherently unstable.

At present in the simulation the algorithm is called at the end of successive integration periods (T) for each unit. In the prototype units we intend to take advantage of the fact that each has its own microprocessor to experiment with alternative approaches - for example recalculating at more frequent intervals than the basic integration period. The problem , of course , is to balance speed of response with smoothing. Also, it should be noted that the measurement of Nc requires the 'capture-switching` capability which is included in the design of the prototype units.

Parameter values:

| | |
|---|---|
| clashcontrol | 4 % |
| T | 100 packet durations |
| Ts min | 1.5 " " |
| Ts max | 120 " " |

Special Scheduler.

This is an event driven scheduler and is invoked by a unit whenever it is in receipt of a packet that requires relaying or final acknowledgement. The special schedule always occurs within a short period of the originating reception and can remove the need to wait for the continuous scheduler which may be operating with long inter-scheduling times. This recognises that it is unnecessary to decouple the system from internal events in the way that it is required for external events. Moreover, by synchronising schedules in this way, we have found it possible to affect a significant reduction of in-system delays whilst simultaneously increasing throughput.

The actual period between the invocation of the special scheduler and the scheduling event that is produced depends on the type of received packet which originated the call. Two categories exist :-

i) Packet received at final unique destination
ii) Any other packet for which an acknowledgement must be transmitted

In the first case we have the advantage of knowing that a single unique unit must send the acknowledgement. Therefore it is reasonable to give it an immediate special schedule. In practice there will be some processing time before such a unit can decide that it is entitled to this privilege and so this is implemented in the simulation as a short constant offset.

In all other cases there is generally the possibility that more than one unit will be entitled to send an acknowledgement and consequently the fixed minimum offset would do no more than guarantee a clash. A typical situation in which several units are equally eligible is when they are all members of the same relaying group. Essentially we would still like to have rapid acknowledgement such that unecessary retransmissions might be avoided but we must also reduce the probability that the acknowledgement is lost in a collision. We have chosen to make use of the ability of such a unit to determine its membership of a relaying group (by reference to its routing data) as a mechanism by which to assign fixed but graduated offsets. The order of the offsets is made to be the same as the ascending unique unit identifiers of all members in the group.

## B. Acknowledgement Strategy

Because of the risk of channel contention (implicit in the use of CSMA) and the uncertain nature of radio links in a dynamic tactical network, positive acknowledgement on a 'hop by hop' basis is a fundamental system requirement. The combined acknowledgment and retransmission strategies must be applied to all packets that need to be reliably transported. This is applied to all user-generated packets ('data packets') but is not applied to control packets which are transmitted on a 'percentage success' basis (the loss of particular control packets is acceptable as long as a reasonable percentage succeed).

Our implementation of the 'hop by hop' acknowlegdgements depends on there being labels within the data packets which identify them uniquely. These are constructed by concatenating a unique pre-assigned unit identity with a local (non-unique) packet sequence number. It is then sufficient for acknowledgement purposes to confirm receipt of a packet by transmitting just its identifier. This has the advantage that the storage of acknowlegements and their use of channel capacity may both be economical. Furthermore, the abbreviated acknowledgements are sufficiently small (of the order of 16 bits) that a number of them may be included in the header of a data packet and transmitted with it at marginal cost. In fact, since it is intended that packet buffers should be available in a range of discrete sizes, the acknowledgements may effectively be transmitted for free if the data and headers do not completely fill the smallest suitable packet. This 'piggy-backing` of acknowledgements means that they may be sent as soon as is possible following the reception of the packets to which they correspond (depending on the scheduler) and also that they may be transmitted more than once. Rapid and repeated acknowlegements are advantageous since they can prevent the unecessary retransmissions which might otherwise occur if a single acknowledgement was either lost or received too late.

A useful enhancement is to include with the unique identifier the 'level` at which it is being sent (the no of hops from the transmitting unit to the packet's final destination). This provides a means by which some unnecessary relays may be quenched.

C. Retransmission Strategy

The combination of the special scheduler and the 'pigybacking` of acknowledgements means that it is possible to support relatively short retransmission time-outs. However , the retransmission strategy must account for the fact that the special schedule may fail to gain access to the channel or may suffer a clash such that the acknowledgement would have to wait for the next schedule (probably from the continuous scheduler). Neighbouring units generally have similar scheduling rates and it has proved effective to rely on the normal scheduling mechanism for spacing retransmissions.

In practice the retransmissions are stored on a queue and must wait for scheduling events in order to have channel access opportunities. A retransmission control procedure is automatically implemented in two ways. Firstly, since the retransmission rate is linked to the scheduling rate, the adaption of the scheduler to high load conditions will also cause the retransmissions to back-off. Secondly the retransmission delay actually incurred depends on the number of packets queued for transmission and in high load conditions the queue will build up and result in a further back-off.

An additional control which has been found to be necessary is the provision of a minimum time-out 'R min'. This is a short offset (15 packet durations or Ts whichever is least) designed to ensure that retransmissions cannot be sent before the receipt of an acknowledgement is reasonably likely. That is , if there is an early first schedule and the minimum time-out has not expired then the retransmission packet remains ineligible for selection.

There is no provision to extend the time-out according to the number of retransmissions that have been made. However , after three retransmissions the 'level` indicator is incremented (see routing section) and at after the seventh the packet is discarded as undeliverable.

## D. Packet Storage and Order of Transmission

Each unit must be abls to store a limited number of data packets so as to allow some degree of buffering for newly entered packets and relay packets. It is also essential to be able to retain packets which may require retransmission (ie all those pending acknowledgement). Data packets are stored on three queues;

1. User input queue
2. Relay queue
3. Retransmission queue

The relay and retransmission queues will sometimes be referred to collectively as the transmission queue.

When a schedule occurs a unit must select the most appropriate packet for potential transmission. At a given time it may have a number of packets on each queue and it will also be able to construct routing update packets. The judicous choice of an individual packet is extremely important as it can have a marked effect on performance. This choice is made according to a simple priority list of packet categories. A given category is deemed unavailable if no packet which belongs to it is currently stored or if specified secondary conditions are not satisfied. At the time of a schedule a unit selects a packet from the highest category which is available. The priority list and secondary conditions (of which the queue controls are described in detail in the next section) are as follows:-

1. Route Update Packet

2. Retransmission Packet with available acknowledgements
   Condition 1: Retransmission packet must be timed-in
   Condition 2: Relay queue control must be satisfied

3. Relay Packet with available acknowledgements
   Condition 1: Relay queue control must be satisfied

4. New user packet with available acknowledgements
   Condition 1: User-Input queue control must be satisfied
   Condition 2: Relay queue control must be satisfied

5. Acknowledgements only

The last category will rarely be reached except in a very lightly loaded network for which there is insufficient traffic to 'piggy-back' the acknowledgements.

## E. Transmission Packaging

To increase the efficiency of channel utilisation a single transmission may in fact comprise of a number of component data packets, a list of abbreviated acknowledgements and possibly a routing control packet (Figure 5).

## F. Queue Controls

As an additional safeguard to channel stability we have found it necessary to include queue control procedures which produce control actions when overload is possible. Packets which require storage can arise from two sources. They can either be new packets generated by the user or they can be packets received from another node which require relaying. Consequently it is necessary to employ two means of queue control.

### User input control

This control is a simple accept or reject decision taken according to the combined length of all the packet queues. If this is less than a preset control constant then new user generated packets are accepted by the system. If it is greater than the control constant then new packets are rejected. The reject decision could include an exchange option whereby high priority packets could enter the system at the expense of an existing but expendable packet.

Control Condition: Combined Queue Length >= User Input Queue Control Limit
Control Action : Reject new input from user

### Relay input control

Relay packets pose a greater control problem since they are internal to the system and have already used system capacity. It would be wasteful, for instance, to reject a packet which had already made one or more successful hops accross the network. However, it is also potentially damaging for an overworked node to accept input which it cannot deal with. For this reason the relay input control is implemented upstream such that the control action affects the sender of the packet. This requires that each node broadcast its current relay queue length within the header of all packets that it transmits. When a node is to transmit a packet which will require relaying it must first determine via which of its neighbours the packet can be routed. It does this by examining both its routing table and also the last routing update received from each neighbour. It then checks its record of notified relay queue lengths for each of these potential relay nodes. If all of these recorded queue lengths are greater than a preset control constant then the transmission must be postponed. Otherwise the transmission may proceed. If postponement occurs then that unit will not be able to remove the relay packet from its own queue. This may result in units further upstream having to postpone their own relays and in this manner back-pressure is exerted on the network as a means of flow control.

Control Condition: Relay Queue Length >= Relay Queue Control Limit
At ALL available relay nodes
Control Action : Postpone transmission of relay packet

**Parameter Values :**

| | |
|---|---|
| User-Input Queue Control Limit | 5 packets |
| Relay Queue Control Limit | 2 packets |

## G. Control Modification : Corrections for Hidden-Terminal Effects

Channel access control is provided by the adaptive scheduler operating with an average scheduling rate , Ts. By modifying the value of Ts on the basis of the monitored channel contention rate the adaptive algorithm attempts to keep this rate at a target value which corresponds to optimal loading. The target value is specific to the non-persistent CSMA protocol and the particular system parameters. However, in certain network configurations the CSMA protocol cannot operate and this target control value is made inapplicable. For this reason it is necessary to employ control modification strategies.

Consider the networks of Figure 6. In each case the central unit has three neighbours but the mutual connectivity of these neighbours differs. In (a) the neighbours are completely inter-connected and may communicate directly with each other (single-hops). In (b and c) they are less connected and some communications can only be effected via the central unit. Finally, in (d) the neighbours are disconnected and they can intercommunicate only via the central unit. Therefore, whilst in (a) the central unit need only send and receive its own packets, in (b),(c) and (d) it is likely to have to deal with a progressively greater number of relay packets. Notice also in (b),(c) and (d) that, because its neighbours are hidden from each other and cannot apply the CSMA protocol, the central unit will observe an unusually high clash ratio. This will cause its scheduler to adapt to a low rate of attempted access despite the fact that it is expected to carry extra traffic. The same results apply if these networks are in fact the local sub-nets which are 'visible` to the central unit.

Now, by analysing the updates from its neighbours, the central unit can easily distinguish these four cases. The following algorithm characterises these and similar networks with an integer which is zero for totally inter-connected neighbours, progressively greater than zero for less connected neighbours and a preset maximum value for totally disconnected neighbours. In view of the fact that the decreasing mutual connectivity of the neighbours is mirrored by an increasing partitioning of the network, this algorithm is named 'Particalc` and the resulting integer the 'Partition factor`.

### Particalc Algorithm

This may be called by any unit and uses information contained within the most recently received routing updates from its neighbours. The call need only be repeated if new updates are received from existing or new neighbours.

The unit counts the number of neighbours Nn. Scanning the updates from these neighbours it surveys all their possible inter-connections and counts the number of 'broken` links (non-existent links), Nb . That is, for each neighbour , i, it scans through the update array i(j) for all other neighbours , j (j<>i), and counts the broken connections as defined by zero entries.

Now, the maximum possible number of single direction links connecting Nn nodes is given by;

$$\text{max links} = Nn ( Nn - 1 )$$

The 'Partition factor` is then given by;

partition factor = (Broken links * Max partition factor) / Max links

= ( Nb * Max partition factor ) / ( Nn( Nn - 1) )

'Max partition factor` is a system-wide constant which serves to scale the Partition factor for use as a control modifier.

Application of the Partition factor

The desired control modification is achieved simply by reducing Ts according to the Partition factor as below:-

Ts <- Ts / (Partition factor + 1)

For totally connected sub-nets the partition factor is zero and Ts is unmodified. For all partition factors greater than zero Ts is reduced and the local scheduling rate is therefore increased. The greatest increase occurs for a 'star` sub-net (Figure 6(d)) when the partition factor is equal to 'Max partition factor`.

It should perhaps be stressed that this is an attempt to correct for secondary effects of 'hidden terminals` (ie the undesired adaption of the scheduler in response to the inevitably increased channel contention). The primary effects (the high packet loss rate and consequent large number of required retransmissions) cannot be corrected for in this way.

Parameter Values

| | |
|---|---|
| Max Partition Factor | 6 |

Further modification according to queue lengths

If the preceding control modification strategy fails to fully compensate for the 'hidden terminal` effect which is suffered by a particular unit then it is probable that its transmission queue will expand continuously. Therefore, a large transmission queue length in a 'hidden` environment is symptomatic of insufficient control modification and, if detected, should instigate further action.

All units whose partition factor is greater than unity (ie all units that are subject to 'hidden terminal` effects) are entitled to make a further control action if their transmission queue length exceeds the preset minimum value 'Min Queue-modifier`. This action is to increase the scheduling rate by the factor 'Queue-modifier` which is derived from the transmission queue length itself. This control modification is detailed below :-

Control Condition : Transmission Queue Length > Min Queue-modifier

Control Action : Ts <- Ts / Queue-modifier

where,

$$\text{Queue-modifier} = \begin{array}{ll} \text{Queue Length} & \text{for Queue Length} <= \text{Max Queue-modifier} \\ \text{Max Queue-modifier} & \text{for Queue Length} > \text{Max Queue-modifier} \end{array}$$

Parameter Values

| | |
|---|---|
| Min Queue-modifier | 1 |
| Max Queue-modifier | 5 |

## V. ROUTING

The basic theme of our approach to the routing problem is that in the environments which we are considering there will be considerable overlap of radio coverage between units of the network so that it is highly likely that more than one station will be capable of relaying a given packet closer to its destination. A further feature of the environment is that there will be a relatively high packet loss rate due to interference and fading which makes it impossible to predict, a priori, which of several possible relay units will receive the packet correctly and be in a position to relay it. Therefore the routing as well as the channel access is essentially 'contention-based' in the manner described below. The main claim that we are making for this algorithm is that it is robust to large scale changes in the connectivity of the units and works well in a high packet loss environment.

There are four parts to a distributed routing algorithm:-

1) A traffic forwarding algorithm based on information from the three functions described below (2-4).

2) A measurement of some network performance parameter.

3) A method of distributing the measurements from (2).

4) a method of calculating from the distributed information possible routes to various destinations.

The description below outlines the basic routing algorithm first and then goes onto described the refinements which have resulted in improved performance under fast changing dynamic conditions.

### A. Traffic Assignment

The mode of operation of the traffic assignment algorithm is illustrated by reference to Figures (7 - 10). These figures depict snaphots of a packet traversing a simple 5 station network. It is assumed that due to the operation of parts (2-4) of the routing algorithm that each station has a distance vector (labelled "routes" in the figures) indicating the number of hops to each of the remaining stations. A destination which is a minimum of n transmission hops from a station is also said to be at "level n" with respect to that destination.

The three main routing related parameters in a packet header are:-

(i) The destination address

(ii) An identifier chosen by the source station

(iii) The distance from the transmitter to the destination.
( the initial transmitter is the source station)

When a station receives a packet not destined for it, it checks to see if it is a smaller distance from the destination than the last transmitter of the packet. If it is, it puts the packet on its relaying queue for subsequent transmission. Referring to the example of Figure 7 , after the initial transmission by station (a) , the packet may be received by two stations (b and c). These stations are at level 2 with respect to the destination, one level lower than the previous transmitter, and they both proceed to relay the packet having changed the level indicator to 2. However it so happened that station (b) gained access to the channel before (c) and as long as this transmission is heard by (c) ,it will remove the packet from its relay queue and take no further action as illustrated in Figure 8 (sidestream termination).

The one level relay station (d) processes the packet in a similar manner until it reaches its destination (Figure 9) The transmission at any level may be used as a hop-by-hop acknowledgement for the previous level (downstream termination). Finally, the destination (e) must make a "level 0" transmission to acknowledge receipt from (d), as illustrated in Figure 10.

The chief merit of this traffic assignment algorithm is that it makes full use of the inherent redundancy of the semi-broadcast mode of operation while still permitting the packet to get to its destination in the minimum number of hops.

Some additional explanation of the operation of the algorithm is in order at this point while detailed discussion of its behaviour when the routing data base information held at the stations is out of date will be deferred to a later section. Firstly, the packet identifier although chosen by the source station in ignorance of those identifiers chosen by other stations, is made globally unique in the network by concatentating it with the identifier of source station. Secondly, it is possible that two or more relaying stations are closer to the destination than the previous transmitter but are out of range of each other (due to local terrain features for example). This will lead to some unnecessary and independent relaying of the packet. However as soon as these different routes coallesce nearer to the destination the the second and subsequent copies of the packet will be discarded. In order to perform this quenching operation on redundant copies, all stations maintain a list of the last ten or so packet identifiers, that they have relayed.

Finally, a traffic assignment algorithm is normally responsible for load splitting i.e. if there are a number of alternate routes to a destination, the load shoud be shared between them to minimze delays and local congestion. An advantage of the traffic assignment algorithm described above is that it performs load splitting automatically. Consider two repeaters both receiving a packet for relaying but one with a long relay queue and the other with a short relay queue. If they both have equal access to the channel the one with the short relay queue will transmit the packet first. This will also be heard by the station with the long relay queue which will than discard the packet. Furthermore if some of the relays have the maximum permitted number on their relay queue they will not take any action on receiving the packet in the first place, while those with shorter queues will append it to their relaying queue.

## B. Connectivity measurement

From the traffic assignment algorithm it is apparent that each node has to determine how many hops away it is from all possible destinations in the network. The basic mechanism it uses to determine these distances is that it identifies those units that it is in direct contact with and from distance information supplied by these neighbours, it computes its minimum distance to all possible destinations, as illustrated in Figure 11. This repeated minimisation algorithm is a modified form of the old Arpanet Routing algorithm[9] and a theoretical analysis of it including convergence proofs can be found in the Abrams and Rhodes[10] paper. In our initial version of the connectivity measurement,the existence of connectivity was based on the reception ofa minimum number of received packets in a given time interval. Thus if a unit was transmitting data packets it did not have to use any of its channel access time in sending connectivity measurement packets. Because a more refined version of the algorithm requires link quality to be determined. Each unit now determines the ratio of the number of packets it receives from a neighbour to the number it transmitted.

C. Route Calculation & Dissemination

Each unit calculates from the distance vectors received from its neighbours the minimum distance to all available destinations. It also uses this minimum distance vector as its routing update which it broadcasts to its neighbours.

In general whenever a unit receives an new update from one of its neighbours which alters its minimum distance vector, it should transmit a new routing update. Furthermore, because of the high packet loss rate, either the unit should obtain an acknowledgement for this update or transmit it frequently enough that all neighbours have a very high probability of receiving it. Unfortunately both these actions could significantly degrade the available throughput. In the initial design routing update transmissions were made on a periodic basis such that any loss of updates due to collisions just delayed the dissemination of connectivity changes. The periods were sufficiently long to prevent more than 25% of the channel capacity being taken by routing updates.

D. Enhancements to Repeated Minimization Hop Count Routing Algorithm

The above algorthm works reasonably well for slowly changing topologies with good quality links. In developing a scheme to cope under adverse EME conditions, there were three observations brought to light by the simulation:-

1)If routing updates are event triggered (i.e. by changes in the network connectivity), rapid changes could cause the whole of the channel capacity to be taken up with routing update transmissions. This can be prevented by placing a maximum frequency on the rate at which any unit can transmit a routing update. Thus an event can only trigger an immediate routing update if one has not been transmitted for at least Tu seconds. Tu is so chosen that even if all units transmitted at the maximum frequency only about 25% of the networks capacity would be consumed. However this means that the network will have to perform routing using out-of-date information.

2)Simulations have shown that the hop-counter based routing scheme still works quite well if the units have a pessimistic picture of the network connectivity. This is because the 'hop counter' information held in the nodes under these conditions holds 'signpost' information as to the direction in which a packet should be relayed. Furthermore a packet proceeeding in this directon may skip unnecessary relays as illustrated in Figures 12 - 14. It is possible that an unnecessary relay operation may occur, say from units (b) or (c) . However in a heavily loaded net, when the packet has to join a relaying queue at the various stations, the dowstream acknowledgement of the optimum relayer d (which appears in the header of its next transmitted packet) has a high probability of supressing relays from all the other relayers, as illustrated in Figure 14.

3)If a single hop network is suddenly converted into a multi-hop network the units will have essentially no information to help in the routing and until new link connectivity assesments have been made and distributed only a very inefficient flooding algorithm will work.

The above observations led us to develop a 'hold down' algorithm which tends to give a pessimistic number for the hops to destinations by using only high quality stable links in the hop counter calculations. However if there are no high quality links for all or part of the route, then poor quality links are used in the hop counter calculations. A route quality factor is used to indicate the number of poor quality links involved.

## E. Enhanced Routing Algorithm

### 1) Connectivity Measurement

All units note from received packets those units which are in radio contact with them and are defined as neighbours. They also measure from the numbers of packets received from that neighbour to the number of packets transmitted by a neighbour a quality for that direction of the link. Note that neighbours that are illuminated by hidden terminals compensate in this ratio for the unavoidable clashes due to this feature.

The link quality measurement is an attempt to predict the quality of a given link over the next routing update period. In its simplest form this estimate is based on the performance of the link during the last such period:-

```
linkquality(i,j) = ( no of pkts rxed by j from i ) * 100/(100-clashratio)
                   ----------------------------------------------------
                               ( no of pkts txed by i )

IF linkquality[i,j]>5/8      then the linkstate(i,j)=0 (good), ELSE
IF 5/8>linkquality[i,j]>1/8 then the linkstate(i,j)=1 (poor), ELSE
IF linkquality[i,j]<1/8      then the linkstate(i,j)=inf (link does not exist).
```

The quality factor of the link is actually a Kalman filter like predicition of the state of the link during the next update period and as such can use weighted past values in the calculation.

### 2)Action on receiving a routing update packet

An update (Figure 15) from a neighbour indicates the number of hops to various destinatons and the quality of the route. (A maximum of 16 hops is allowed and each hop has either a 0(good) or 1(poor) quality indicator associated with it; thus 4 bits indicate the number of hops and 4 bits indicate the quality of the route).

a) The entry for the receiving unit in the update is examined to see if the neighbour received the unit's last update. If it did not it sets the 'transmit update flag'.

b) The unit uses the update to recalculate routes to all other stations choosing the minimum hop indications of the highest quality routes. It notes whether any of the route distances or their qualities have changed. If they have changed the unit will broadcast the new update at the earliest opportunity. However if it has not broadcast an update for Tu (routing update control period) seconds it sends out the new update immediately.

3) Action when unit is idle

If a unit does not have any data packets to send over a routing control period, it forces the sending of routing update every Tu seconds in order to alert its neigbours to its continued existence.

4) Action when routing information is incorrect

As mentioned above the rapidity of connectivity changes and the limited rate at which they may be distributed through the network causes the routing information at various nodes to be both out-of-date and inconsistent. As we have seen above, if a unit has a pessimistic measure of the number of hops to a destination this does not cause a problem for the traffic forwarding algorithm, although some unnecessary relaying may be involved. However if a node has too low a value for the distance to the destination then the relayer may not accept the packet for relaying. This problem is overcome by increasing the value of the hop counter in the packet header if no acknowledgement is received after three transmissions. If after seven total transmissions no acknowledgement is received, the unit discards the packet.

## VI. ERROR CONTROL

As has been stated above the error rates experienced even in a benign mobile environment are relatively high , ranging from 1 in a 1000 to 1 in 10. Furthermore the error rates in a hostile tactical environment including the posssible existence of substantial numbers of frequency hopping transmissions may be even higher, upto 1 in 3. Thus strategies will have to be developed for operating in high error rate environments. Because of the quantum nature of the data transfers, ie a few thousand bits per burst, it is necessary to use forward error correction rather than pure error detection and automatic request for repeat (ARQ). A recent study of forward error correction techniques on high error rate channels showed that a good strategy involves using repetitions to get the error rate down to a few percent and then to use a powerful half rate code to reduce the error rate to about 1 in 100000. At this level 99% of the packets can be decoded correctly and further coding is not cost-effective. However the use of a cyclic redundancy check to indicate the success or otherwise of the decoding is essential. This ensures that the probability that a message is presented to the user as correct, when in fact it is not, is less than 1 in 1000,000,000. If the decode fails then the transmitter will not receive an acknowledgement for its packet and will retransmit it. One of the open questions in operating in a variable error rate environment is what sort of adaptive coding algorithm can be used which will optimize the use of the link quality.

Unfortunately the performance of the powerful error correcting codes is severely degraded by bursts of errors. This problem is overcome by interleaving at the transmitter and de-interleaving at the receiver. An important parameter of the interleaving is its 'depth',which determines how large a burst is completely broken up before entering the decoder. In synchronous communications the depth of interleaving is limited by the acceptable delay and memory size of the interleaver/deinterleaver. However in burst transmission systems it is limited to the square root of the depth of the message. Thus the amount of interleaving applied may vary with packet length.

There are a number of powerful coding techniques with their associated decoders due to Bose, Chadhuri and Hochenheim, Viterbi, Jelinek and Fano. These algorithms can be implemented on general purpose microprocessors but will only operate upto a few hundred bits per second. Special purpose hardware is required for decoders operating at higher speeds.

## VII. PERFORMANCE

The RSRE Packet Radio simulator fully implements all the algorithms described above, independently for each unit in the network. A two dimensional connectivity matrix is used to determine which units are affected by the actions of current transmitters.

Hundreds of hours of simulations have been performed on networks with various loadings, topologies and control parameter settings. A major aspect of these results has been that, although performance is sensitive to the choice of algorithm, it is not particularly sensitive to the exact setting of any parameter values. The main criteria which affect the throughput and delay of such networks will be summaraized followed by the particular throuhgput/delay performance of a network subjected to rapid and large changes in connectivity.

The main parameters used in the simulations to which the results refer are:-

| | | |
|---|---|---|
| run time | 2,000,000 | units |
| packet duration | 100 | " " |
| rx to tx switch time | 5 | " " |
| tx to rx switch time | 5 | " " |
| capture switching | 'ON` | |

The percentage loadings and throughputs referred to below and illustated in Figure 16 are obtained by dividing the total number of delivered bits by the channel bit rate multiplied by the time of the simulation. Thus percentages do not include header or coding overheads.

In one way the figures are pessimistic in that acknowlegment packets where used are the same sise as data packets. Under high loading conditions most acknowledgements are piggybacked.

When using the distributed channel access, routing and network control algorithms, as described above, the performance in terms of throughput , delay and delay dispersion is relatively insensitive to the exact setting of their parameters. This should contribute to the overall stabilty of the network and certainly the simulation appears to confirm this. Otherwise the performance is efectively determined by a few crucial parameters:-

1. 'Carrier Sensing' Time

The first critical parameter is the ratio of the 'carrier sensing' dead time to the average packet duration. A major contributor to this time being the receive-to-transmit switching time of the transceiver. The effect of this dead-time can be predicted from the Kleinrock and Tobagi curves [2] for CSMA performance.

2. Connectivity

The actual connectivity at a given time and the rate of change of connectivity are both important parameters. The former affects the amount of relaying which is required and determines the number of 'hidden terminals' whilst the latter affects the volume of control information to be exchanged and also the accuracy of routing tables.

3. Loading

The traffic loading and distribution both affect the network performance. To date the generation of source to destination pairs has been random and we have not experimented with uneven loadings. The overall input rate determines the operating point on the CSMA performance curve until it limited by the input control. Consequently the delays are significantly less at low input rates.

Performance with Single-Hop topologies

The 'single-hop` or fully connected network is a special topological case which has significantly better throughput/delay characteristics than others. It obtains full benefit from the cooperative properties of CSMA. When traffic is offered randomly by all users , acknowledged throughput rates of about 60% channel capacity are achievable neglecting header and coding overheads. This figure is sensitive to the action of the 'special scheduler' which permits any unit which has just received a packet for acknowledgement an immediate channel access opportunity. It has been noted that most transmissions are successful on their first attempt and therefore the average delivery time from first transmission is of the order of a few hundred msds. However in a heavily loaded network packets will suffer significant pre-transmission delays. The throughput figures have been roughly translated into messages/hour, (by assuming an 80 byte message, 20 byte packet radio header and half-rate Forward Error Control coding overall), in Figure 16.

## Performance with Multiple-Hop Topologies

Although throughput/delay performance for multiple hop networks depends upon offered traffic patterns and topology, simulations have shown that for random traffic patterns and topologies with reasonable numbers of relayers that the main factor affecting performance is whether or not the topology is static. This effect is quite easily explained. The dynamic changes have two effects:-

i) They cause the network to attempt to route packets when the routing data base information is out-of-date and/or inconsistent The algorithms to circumvent these problems involve extra transmissions.

ii) Routing updates which take up some of the channel capacity are only transmitted when changes occur.

Apart from the dynamics of the topology, the maximum throughput and delay are relatively independent of topology. The main reason for this appears to be that as the connectvity becomes more cellular more units can transmit simultaneously without causing collisions, and thus there is some frequency reuse in non-adjacent areas of connectivity. Acknowledged throughput rates in the range 25-36% have been achieved in the static multiple-hop topologies.

## Performance with Dynamic Topology

The results from the simulations in which rapid connectivity changes have been induced have been most promising. Basically the link quality assessment time constants are related to the known time that it takes updates to to be disseminated. So unless the connectvity measurements indicate that the link is going to be available for a useful period of time, it is not included in the minimum distance calculation.

Thus the routing tables reflect a pessimistic view of the number of hops required, but when the shorter hop routes are available, the contention based routing algorithm permits them to be used.

As an illustration of the performance of a network under extremely unfavourable conditions we have taken the case of a 25 unit network where the connectivity can be varied between a 2-hop (good) and 5-hop (bad) scenarios, as shown in Figure 17. The simulation has caused the connectivity to switch between these two states at rates between once every 50 time units (half a packet time) and once every 100,000 time units. It can be seen from the time constants indicated in the routing algorithm that for most of these switching times routing information cannot be distributed from one end of the network to the other! The ratio of the time spent in the good and bad states is the same for all simulation runs so that the results can be compared. The ratio used in the example is 25% in the good state and 75% in the bad state, but the results are maintained for all ratios. Figure 18 illustrates the throughput, average delay and lost packets for various accepted loads. The lost packets are those which fail to arrive at their destination because some where along the route a unit has transmitted them seven times but because of confusion in the routing tables has found no 'nearer' unit to accept and relay them. The figures correspond to acknowledged throughput rates of about 15%. On a 16kbit/s channel this corresponds to 6000 eighty-byte packets per hour including coding and header overheads. Note that the quoted message throughput rate is for the basic "unreliable datagram" service which uses hop-by-hop acknowledgement only.

## VIII. PROTOTYPE PACKET RADIO STATION EQUIPMENT

A simple three station network, based on the equipment illustrated in Figure 19, is in the process of being built. This mini-network will be used to establish the elemental behaviour of Packet Radio operation including the link performance of the burst transmission scheme and the effects on a receiver of collisions in the CSMA environment. Results from experiments with the mini-network will fed back into the simulation to ensure that its predicted results for a large network are as realistic as possible.

The hardware of the prototype equipment is composed of three units:-

1) The radio transciever

2) A Data Radio Interface Unit (DRIU) which performs baseband signal processing, timing extraction, start of message recognition, error control and other tasks not cost-effectively performed by a general purpose micro/minicomputer.

3) The main general purpose processor which controls 1 and 2 and implements networking protocols and user interface functions.

As has been mentioned above, the ability to use an existing voice radio as the basis for a Packet Radio station is extremely attractive. It was decided that in the first stage of Packet Radio development to choose this particular strategy. The first prototypes will employ a 16 kbit/sec VHF voice transceiver. A critical parameter of the radio transceiver is its receive-to-transmit switching time for reasons stated above. Fortunately the transceiver under consideration has a very short receive-to-transmit switching time for a voice radio. This is mainly due to the fact that its local oscillator does not change frequency when the set changes modes. The receive-to-transmit switching times have been measured on the bench to be approximately 4 milliseconds. With packet duration times of 62.5, 125 and 187.5 milliseconds, an average switch to packet duration time ratio of about 5-8% may be achieved.

An important part of the design of our medium speed network is the assumption that all nodes will be able to process fully all packet headers. In order to be able to process upto 16 packets a second and perform all the necessary accesses and changes to the data structures at each station, the main station processor must have a wide bandwidth I/O port to the DRIU which does not consume more than a nominal portion its capacity. Thus this interface is a direct memory access (DMA) type in which the processor only has to set up address and counter registers at the begining of a transfer and it is interrupted when the transfer is complete.

The DRIU unit incorporates forward error correction coding and interleaving with the facility for code rates of 1, 1/2, 1/6, and 1/10. The latter low rate codes employ repetitive coding to bring the error rate down to < 5% which are then further reduced by the half rate convolutional code. The half rate code is a convolutional code of constraint length 48 [11] which is decoded using sequential decoding. The sequential decoder has sufficient processing power to perform 64 computations per decoded bit. This is more than adequate for normal requirements as the number of computations per bit increases exponentially at high error rates and there is little to be gained by increasing the processing power over the stated value. The interleaving is performed to depth 32. Thus a block of 32 errors would arrive at the decoder evenly spaced over 1024 bits, greatly easing the work of the decoder.

The DRIU also incorporates twin demodulator circuitry for evaluation of capture switching strategies.

The PDP-11/23 was chosen as the main station processor, because the Communications Group has a special real-time operating system for this machine which takes advantage of its memory management facilities to have access to 256 kbytes of main memory [12]. Furthermore internetworking and gateway protocols have been developed for this machine which can be used in the base station of the network [6]. Although it provides considerably more processing power than is necessary, a great convenience during development, the 11/23 is also part of a family of processors some of the less powerful members of which could be used in a production equipment.

## IX. CONCLUSION

A fully distributed approach to the design of a Packet Radio network has been described. The algorithms which we have developed have been influenced by the highly mobile and hostile nature of the evironment in which systems will be expected to operate. Detailed simulations have been used to evaluate the performance and stability of the algorithms. The channel access and network control strategies as currently implemented are capable of maintaining a useful grade of service over a wide range of operating conditions. In particular, the routing algorithms have been shown to provide a very acceptable level of service when more orthodox algorithms would be generating unsupportable overheads. Further work will include refining and enhancing the robustness of the channel access and routing algorithms in conjunction with real connectivity measurements from the field.

## X. REFERENCES

1. KAHN R E, GRONEMEYER S A, BURCHFIEL J & KUNZELMAN R C,
"Advances in Packet Radio Technology",
PROC IEEE Vol 66 No 11, pps 1468 1496 Nov 1978.

2. KLEINROCK L & TOBAGI F, "Packet Switching in Radio Channels:
Part I - Carrier Sense Multiple Access Modes and their Throughput and Delay Characteristics."
IEEE COMMS Vol 23, No 12 , pgs 1400-1416 Dec 1975.

3. TOBAGI F A & KLEINROCK L, "Packet Switching in Radio Channels:
Part II - Hidden terminal problem in Carrier sense multiple access and the busy tone solution."
IEEE Trans Comms Vol 23, no 12, pg 1417-1433 Dec 1975.

4. TOBAGI F A & KELINROCK L , "Packet Switching in Radio Channels: Part IV - Stability considerations and Dynamic Control in Carrier Sense Multiple Access", IEEE Comms Vol 25 No 10, pgs 1103-1119, Oct 1977.

5. LEINER B M, "A Simple Model for Computation of Packet Radio Network Performance" IEEE Comms Vol 28, No 12 , pgs 2020-2023, Dec 1980.

6. DAVIES B H & BATES A S, "Internetworking in the Military Environment", Proc IEEE INFOCOM 82 Conf, pps 19-29, Las Vegas, March 1982.

7. DARPA , "DOD Standard Transmission Control Protocol" Defense Advanced Research Projects Agency, IEN-129, Jan 1980.

8. DARPA , "DOD Standard Internet Protocol" Defense Advanced Research Projects Agency, IEN-128, Jan 1980.

9. McQUILLAN J M, FALK G & RICHER I, "A Review of the Development of the ARPANET Routing Algorithm" IEEE Comms Vol 26, No 12, pgs 1802-1811, Dec. 1978.

10. ABRAM J M & RHODES I B, "Some Shortest path Algorithms with Decentralised Information and Communication Requirements", IEEE Aut Contrl, vol 27, no 3, pgs 570-582, June 1982.

11. FORNEY C D & BOWER E K, "A High Speed Sequential Decoder", IEEE COMMS Vol 19, No 5, p821-, Oct 1971.

12. WISEMAN S R & DAVIES B H, "Memory Management Extensions to the SRI Micro Operating System for PDP - 11/23/34/35/40" ARPA Internet Experimental Notebook, IEN-136, May 1980.

## XI. LIST OF ILLUSTRATIONS

Figure

1 Basic Concepts of Packet Radio

2 Packet Radio - System Design Considerations

3 Schematic of Continuous Scheduler

4 Dependence of Adjustment to Scheduling Interval (T) on Current Value

5 Transmission Packaging

6 Adaptive Scheduling Modification for Hidden Terminal Effects

7 Normal Routing - Snapshot 1

8 Normal Routing - Snapshot 2

9 Normal Routing - Snapshot 3

10 Normal Routing - Snapshot 4
11 Routing Database Held at Node (c)
12 Routing with Out-of-Date Tables - Snapshot 1
13 Routing with Out-of-Date Tables - Snapshot 2
14 Routing with Out-of-Date Tables - Snapshot 3
15 Format of Routing Update Packet
16 Throughput Performance
17 Two Connectivity States used in Dynamic Perfomance Evaluation
18 Performance of Dynamic Multiple-Hop Topology of Figure 17
19 Flexible Prototype Tactical Data Station

BASIC CONCEPTS OF PACKET*RADIO

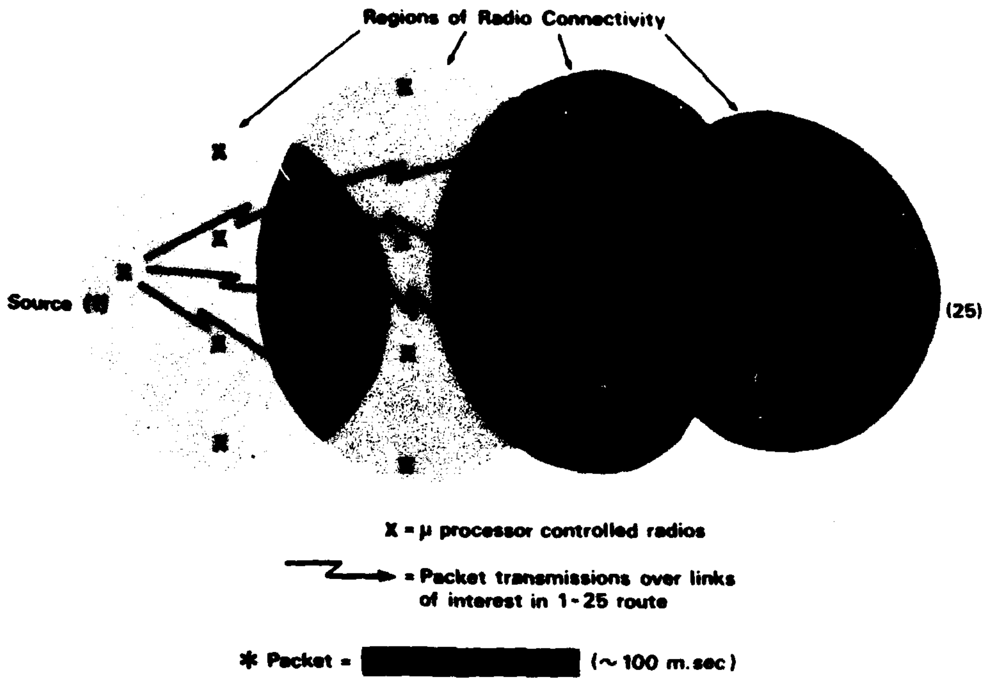

Regions of Radio Connectivity
Source (1)
(25)
X = μ processor controlled radios
= Packet transmissions over links of interest in 1-25 route
* Packet = (~100 m.sec)

Fig I Basic Concepts of Packet Radio

PACKET RADIO-SYSTEM DESIGN CONSIDERATIONS

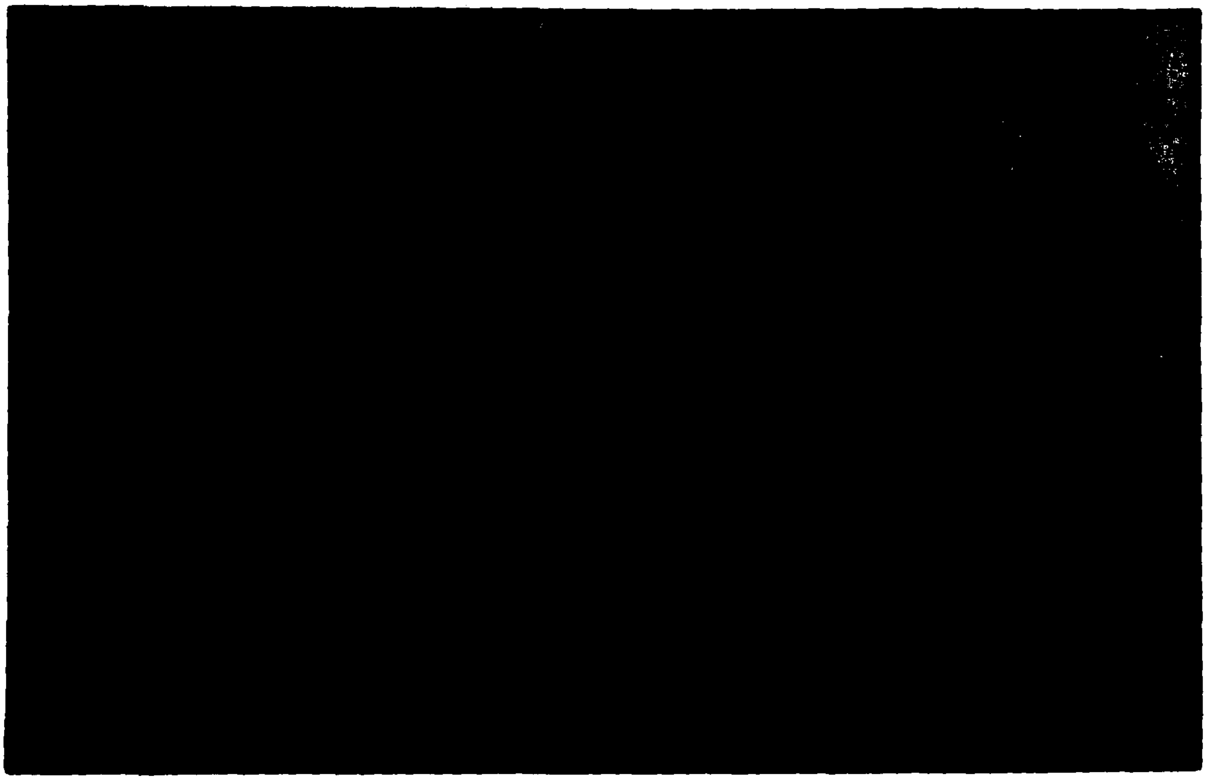


Fig 2 Packet Radio – System Design Considerations

Fig 3 Schematic of Continuous Scheduler

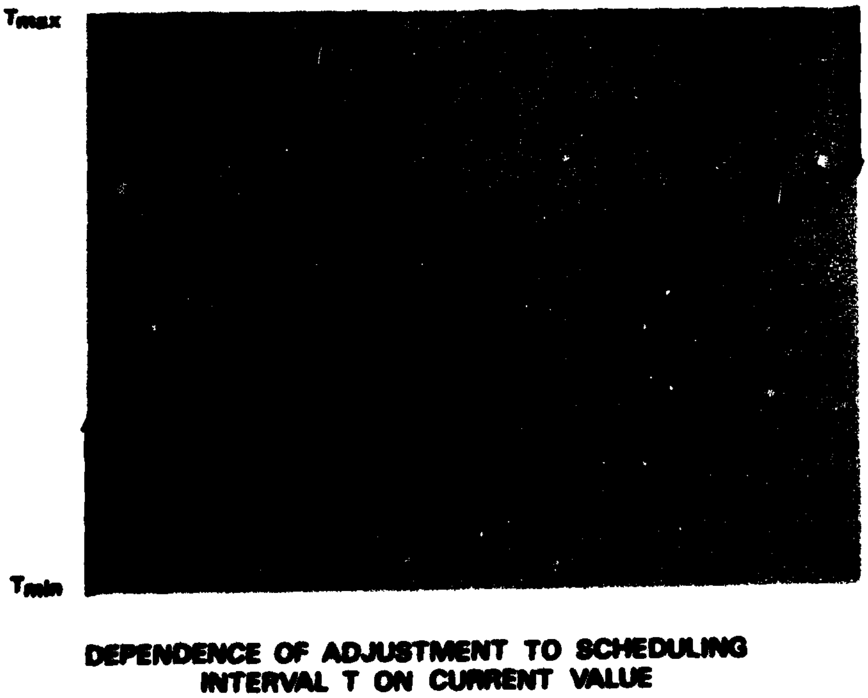


Fig 4 Dependence of Adjustment to Scheduling Interval (T) on Current Value

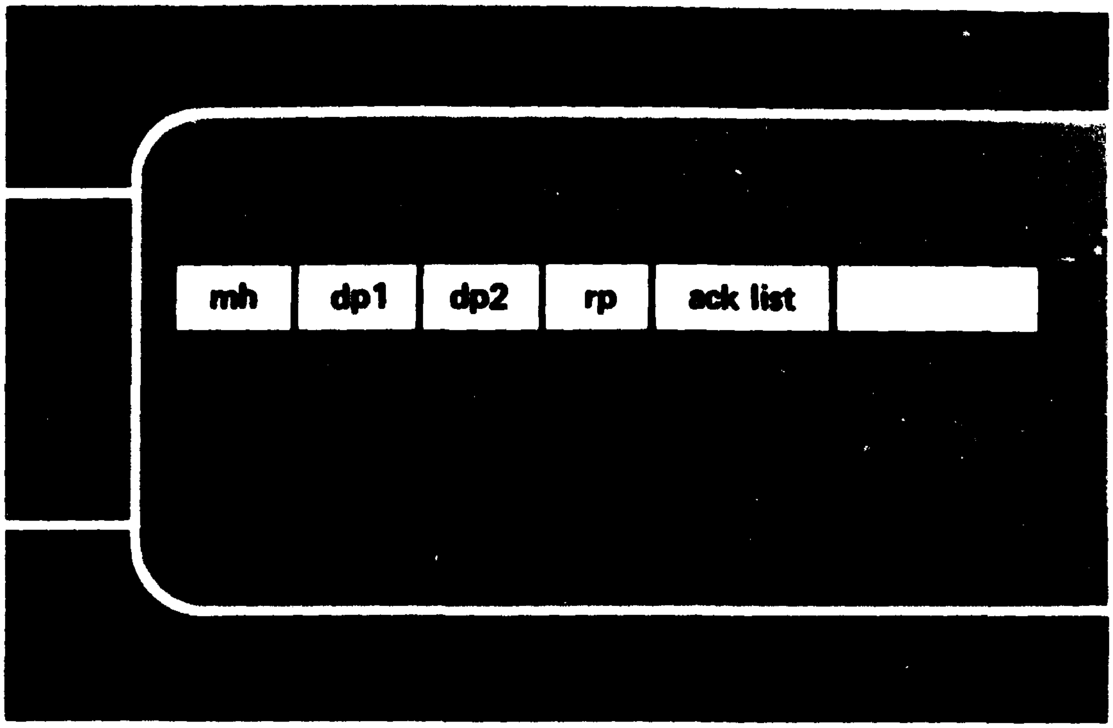
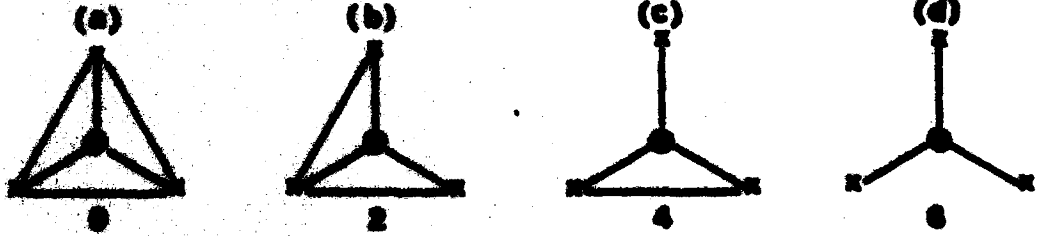


Fig 5 Transmission Packaging

## CONTROL MODIFICATION

Nt total possible neighbour – neighbour links
Nm number of missing links

Partition Factor = (Nm/Nt) x Max Partition Factor



Modification of Scheduling rate

Ts = Ts / (Partition Factor + 1)

Fig 6 Adaptive Scheduling Modification for Hidden Terminal Effects

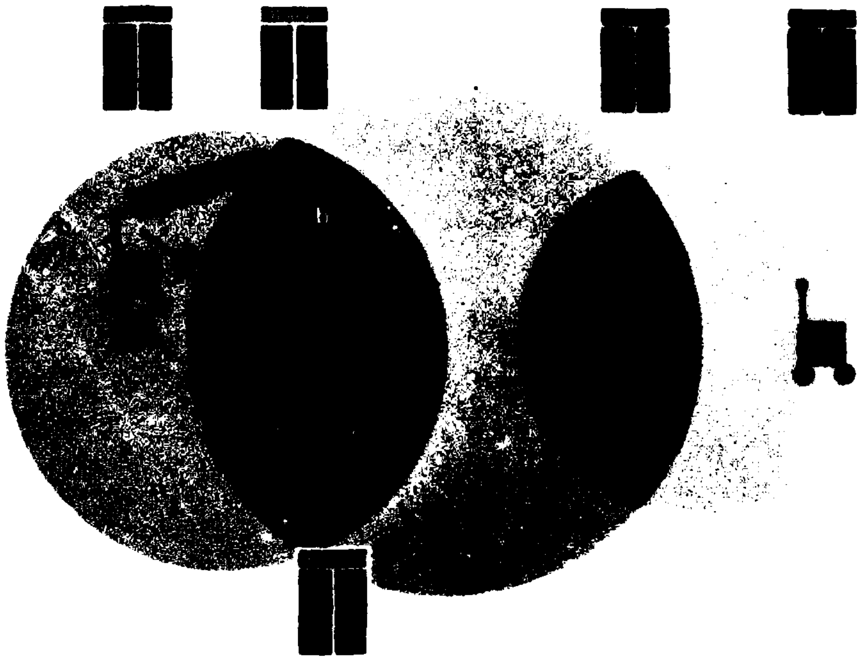


Fig 7    Normal Routing – Snapshot 1

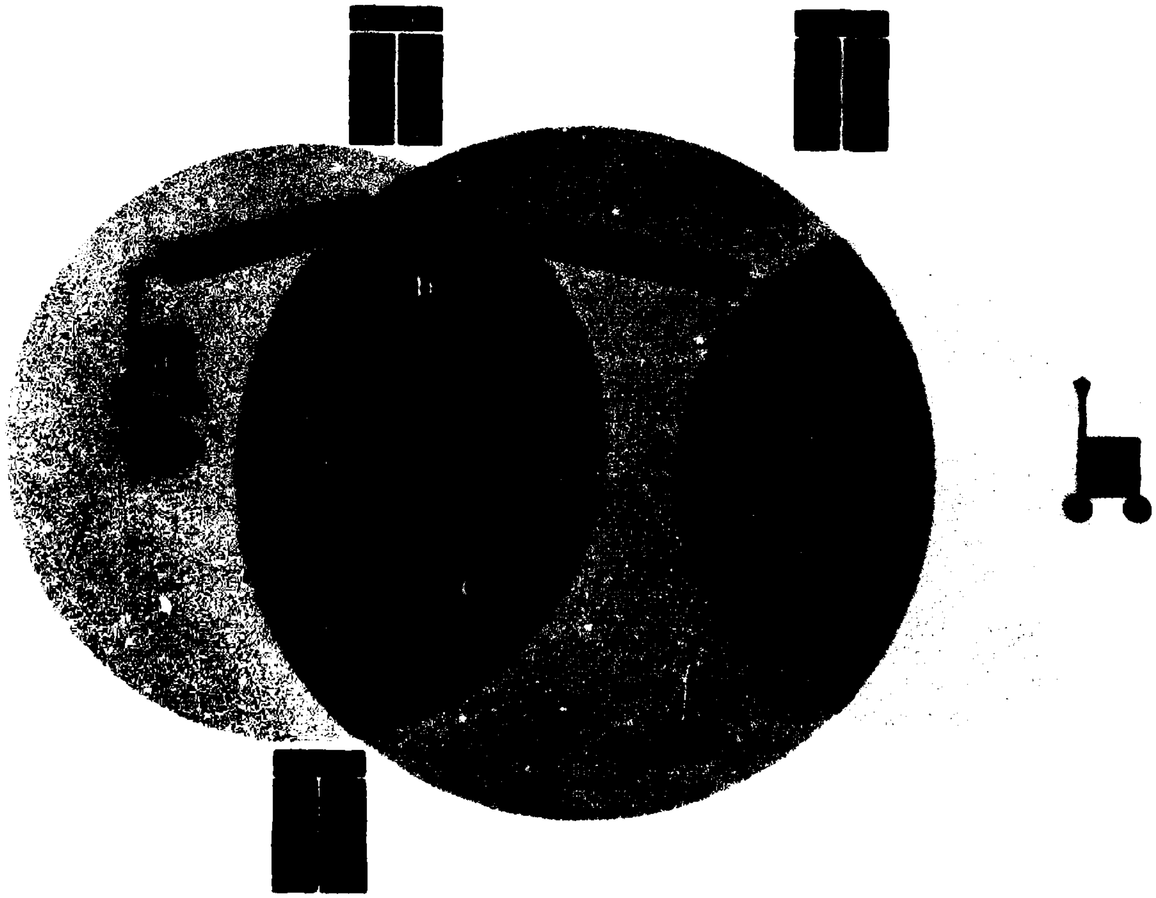


Fig 8    Normal Routing – Snapshot 2

Fig 9 Normal Routing – Snapshot 3

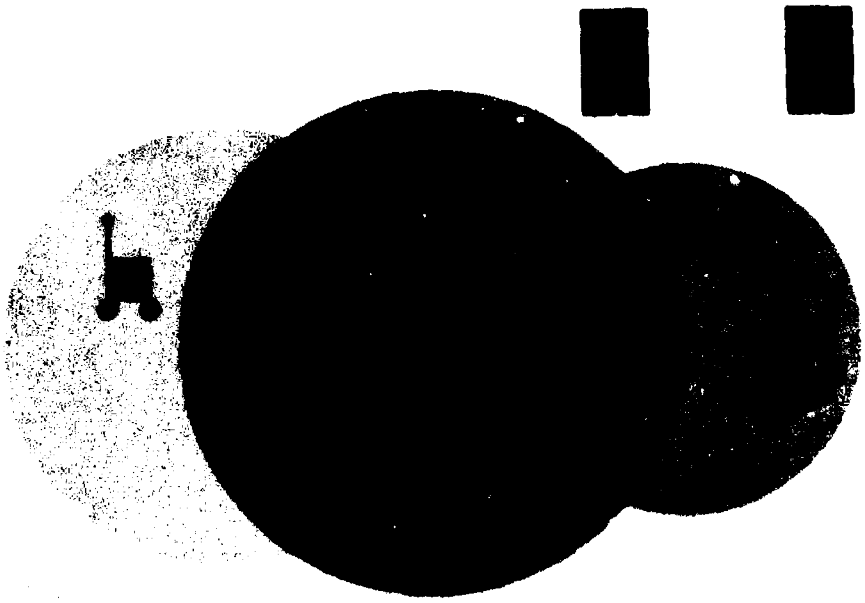
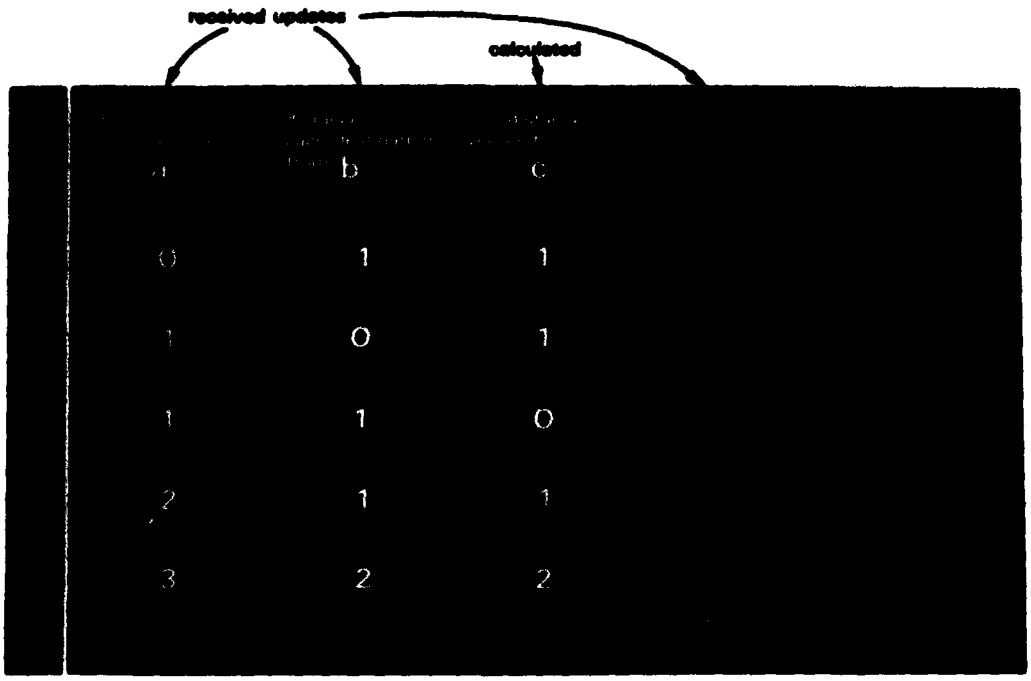


Fig 10 Normal Routing – Snapshot 4


received updates
calculated

| a | b | c |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |
| 2 | 1 | 1 |
| 3 | 2 | 2 |

**ROUTING DATABASE HELD AT NODE C**

Fig 11 Routing Database Held at Node (c)

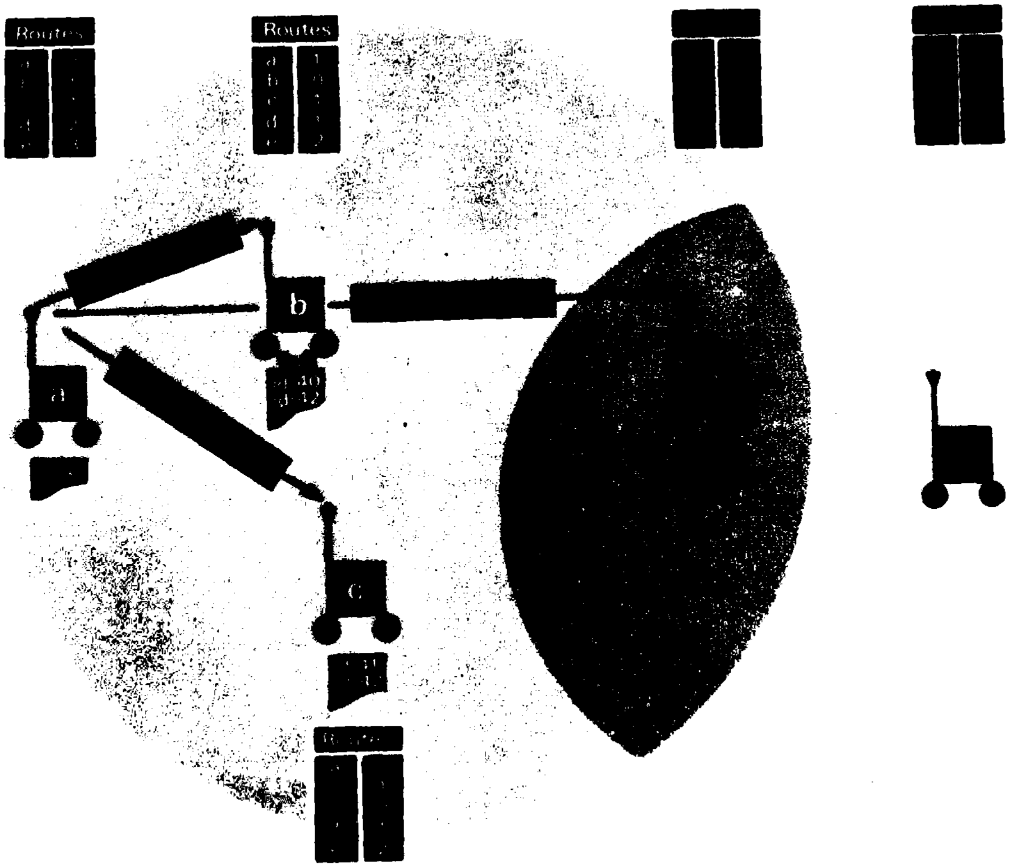


Fig 12 Routing with Out–of–Date Tables – Snapshot 1

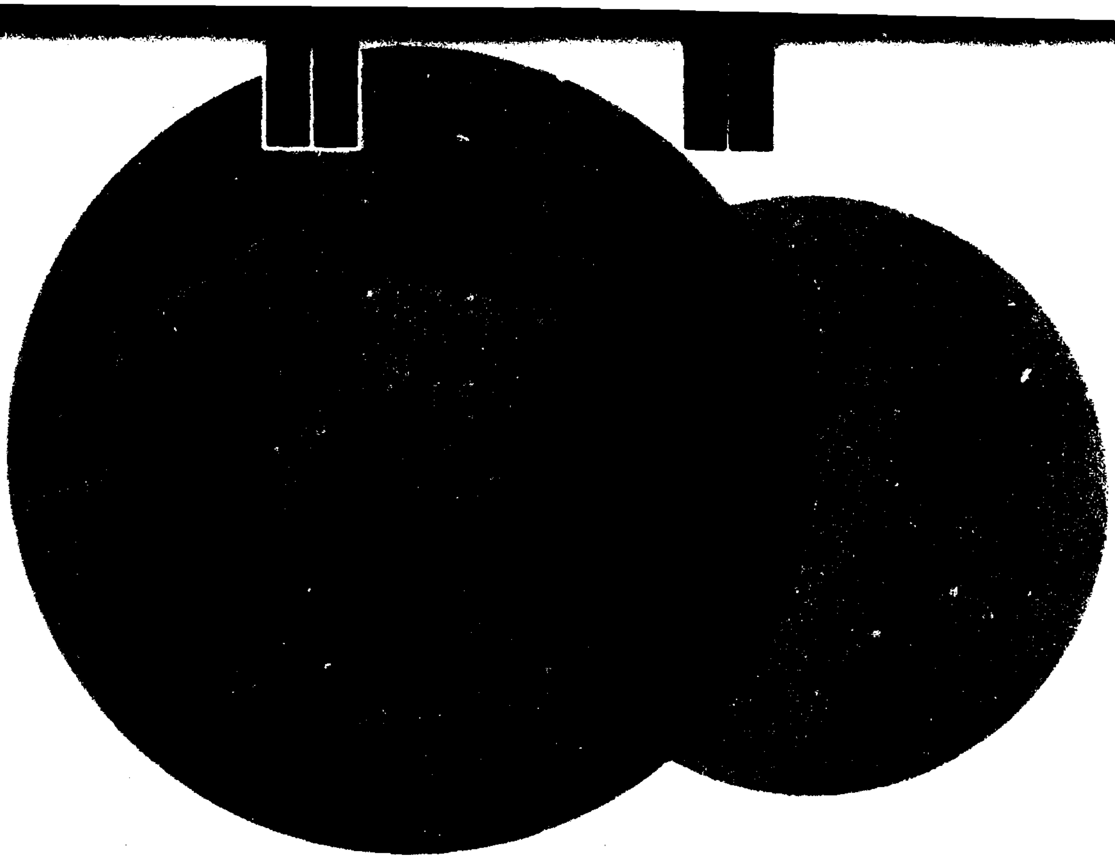


Fig 13 Routing with Out–of–Date Tables – Snapshot 2

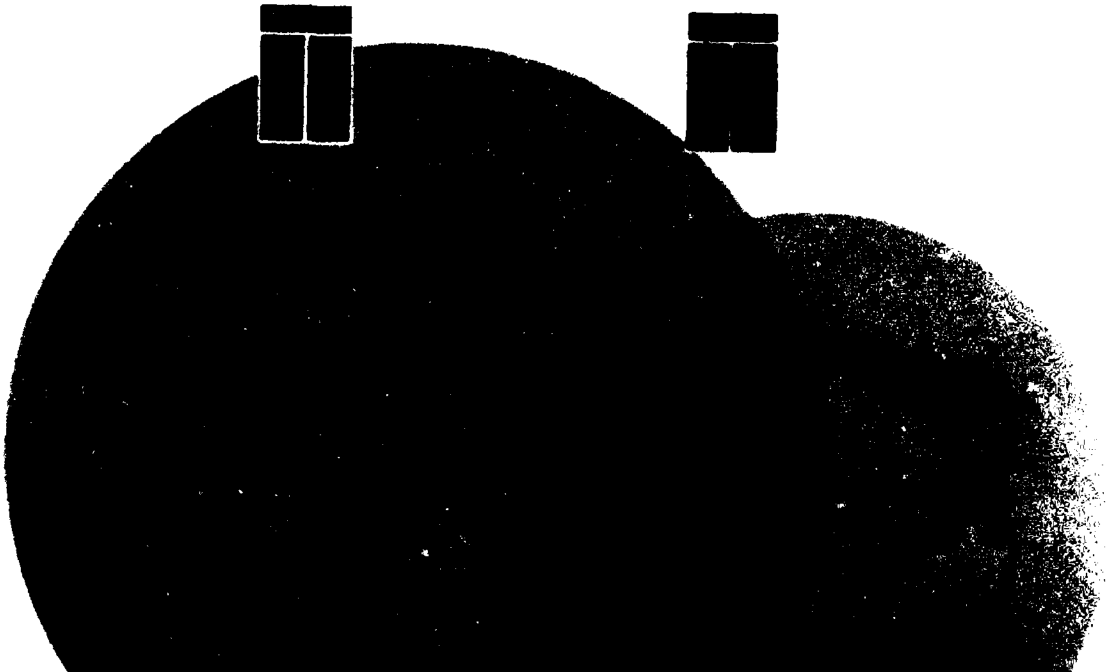


Fig 14 Routing with Out–of–Date Tables – Snapshot 3

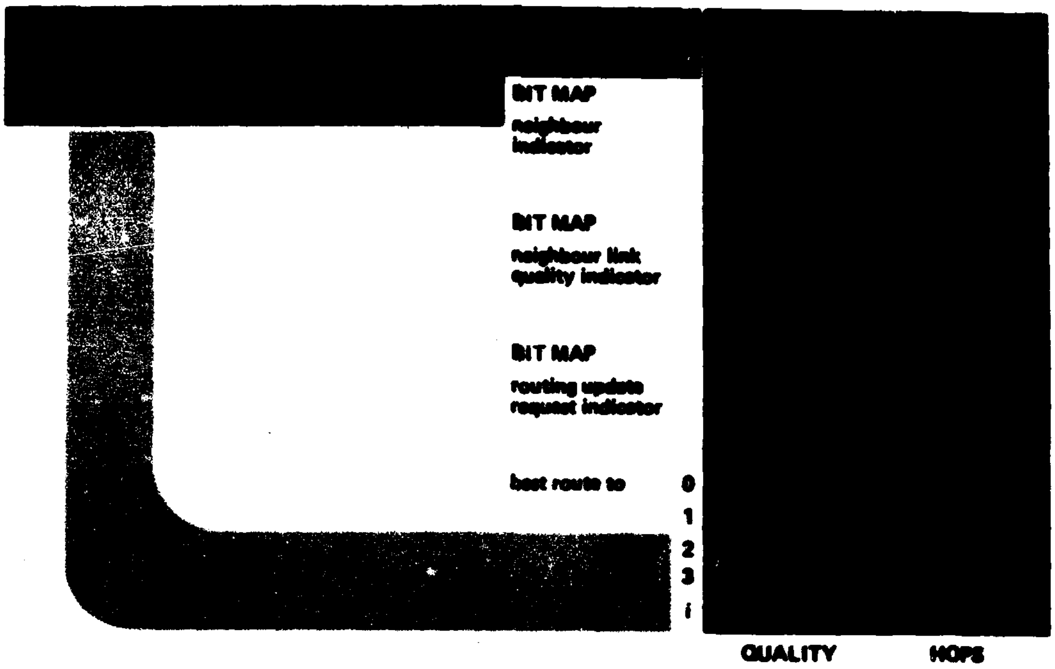
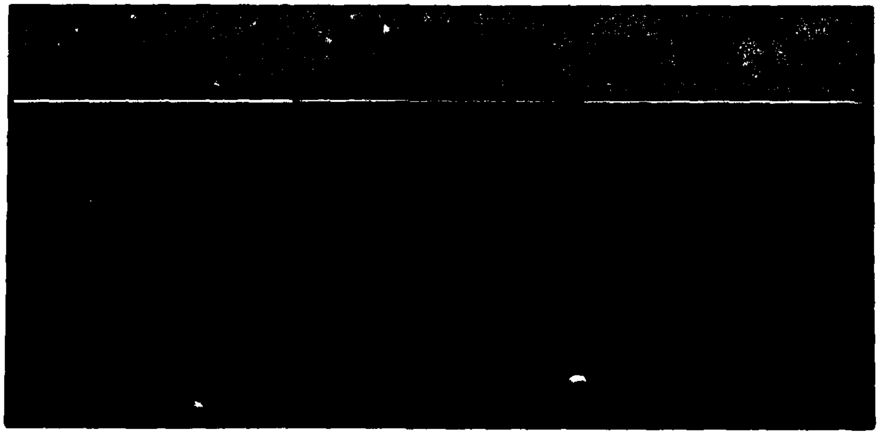


Fig 15 Format of Routing Update Packet

## THROUGHPUT PERFORMANCE

$a^{\dagger} = 0.05$



$^{\dagger}a = \frac{\text{carrier sensing dead time}}{\text{average packet duration}}$

Fig 16 Throughput Performance

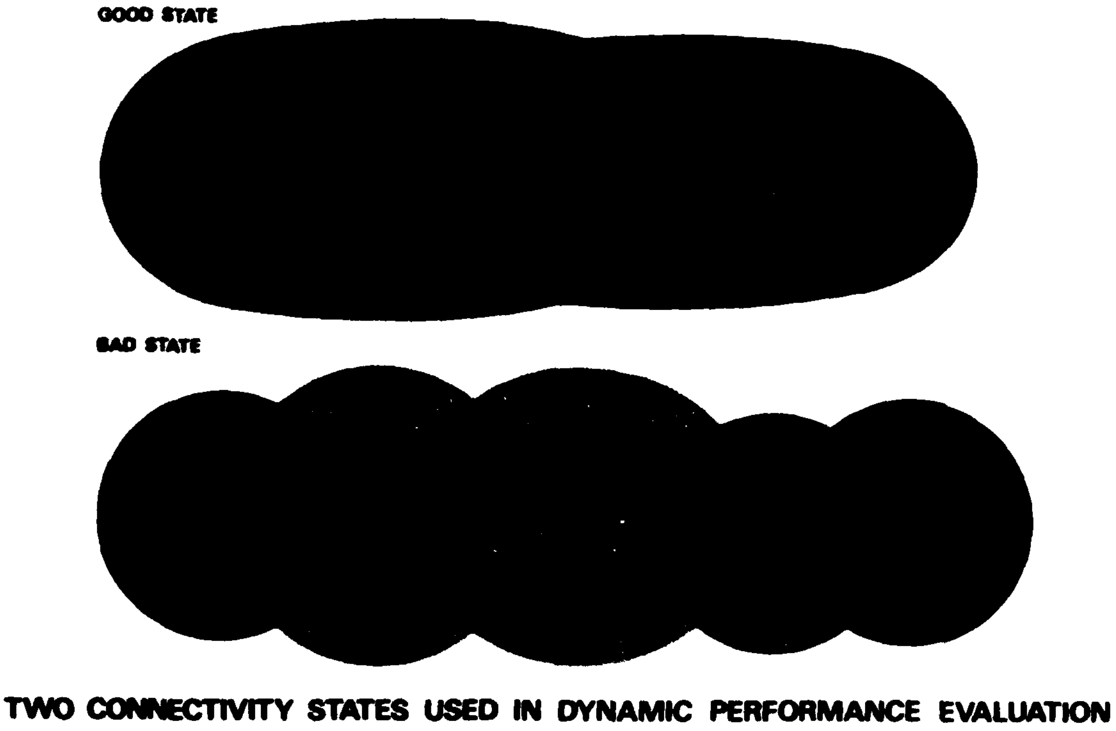

GOOD STATE
BAD STATE
TWO CONNECTIVITY STATES USED IN DYNAMIC PERFORMANCE EVALUATION

Fig 17 Two Connectivity States used in Dynamic Performance Evaluation

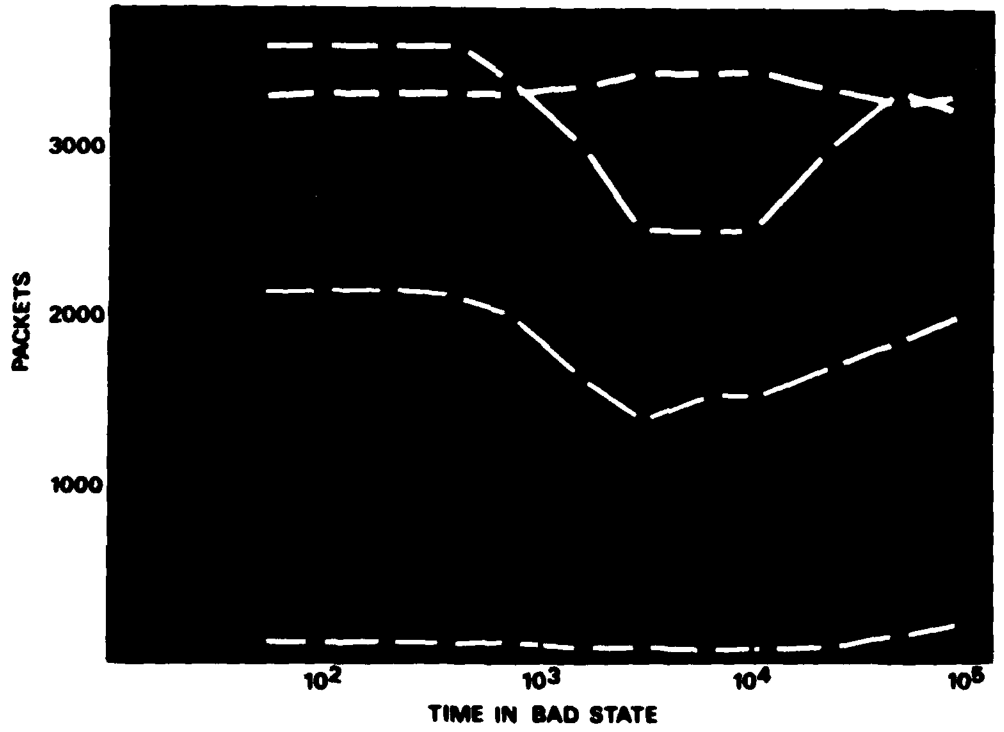
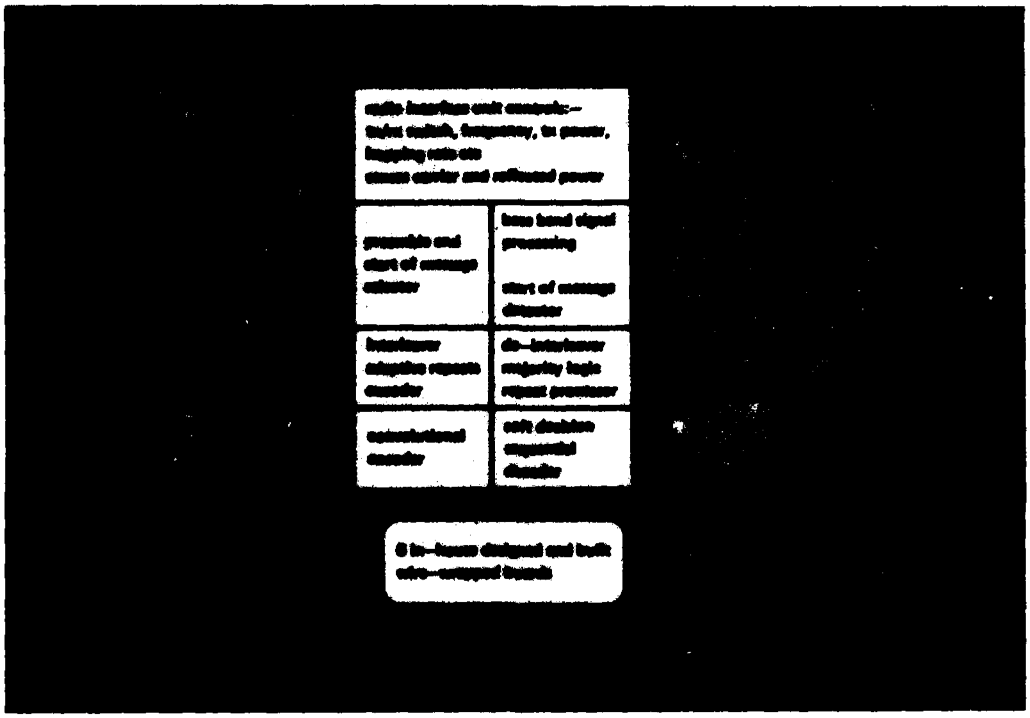


Fig 18 Performance of Dynamic Multiple–Hop Topology of ⁼igure 17



radio interface unit controls— [illegible] switch, frequency, tx power, keying rate etc [illegible] carrier and reflected power

preamble and start of message selector

base band signal processing

start of message detector

interleaver adaptive repeats encoder

de—interleaver majority logic repeat processor

convolutional encoder

soft decision sequential decoder

8 in—house designed and built wire—wrapped boards

Fig 19 Flexible Prototype Tactical Data Station

## DOCUMENT CONTROL SHEET

Overall security classification of sheet UNCLASSIFIED

(As far as possible this sheet should contain only unclassified information. If it is necessary to enter classified information, the box concerned must be marked to indicate the classification eg (R) (C) or (S) )

| | | | |
|---|---|---|---|
| 1. DRIC Reference (if known) | 2. Originator's Reference<br>REPORT 84003 | 3. Agency Reference | 4. Report Security Classification<br>U/C |

| | |
|---|---|
| 5. Originator's Code (if known) | 6. Originator (Corporate Author) Name and Location<br>ROYAL SIGNALS AND RADAR ESTABLISHMENT |
| 5a. Sponsoring Agency's Code (if known) | 6a. Sponsoring Agency (Contract Authority) Name and Location |

7. Title

A FULLY DISTRIBUTED APPROACH TO THE DESIGN OF A 16 KBIT/SEC VHF PACKET RADIO NETWORK

7a. Title in Foreign Language (in the case of translations)

7b. Presented at (for conference papers) Title, place and date of conference

| | | | | |
|---|---|---|---|---|
| 8. Author 1 Surname, initials<br>HAZELL, M S | 9(a) Author 2<br>DAVIES, B H | 9(b) Authors 3,4... | 10. Date | pp. ref. |

| | | | |
|---|---|---|---|
| 11. Contract Number | 12. Period | 13. Project | 14. Other Reference |

15. Distribution statement

UNLIMITED

Descriptors (or keywords)

continue on separate piece of paper

Abstract

System design considerations for a Packet Radio network operating in the mobile tactical environment are outlined. Survivability is assessed to be of primary importance and a fully distributed approach in which all nodes are functionally equivalent and the network self-configuring is favoured. Emphasis is placed on a description of the channel access (CA), routing and congestion control algorithms. The CA algorithm is an adaptive CSMA scheme which is designed to maintain good throughput-delay performance irrespective of the number of active users and offered loading. It specifically includes features which compensate for 'hidden terminal' effects in multiple hop networks. The routing strategy takes advantage of the inherent path redundancy of the semi-broadcast environment to offset the high packet loss rate due to collisions, interference and

... cont.

ATE

LMED

-8